REMARKS/ARGUMENTS

This Amendment is in response to the Office Action mailed June 18, 2007.

In the Office Action, the claims 1, 4, 9-14, 17, and 22-26 stand rejected under 35 U.S.C. § 103.

Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 103

Claims 1, 4, 9-14, 17, and 22-26 stand rejected under 35 U.S.C. § 103(a) as being allegedly obvious over U.S. Patent No. 6,385,729 issued to DiGiorgio et al. (hereinafter DiGiorgio) in view of U.S. Patent No. 6,038,551 issued to Barlow et al. (hereinafter Barlow).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *MPEP §2143, p. 2100-126 to 2100-130 (8th Ed., Rev. 5, August 2006).*

Furthermore, the Supreme Court in *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966), stated: "Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined." MPEP 2141. In *KSR International Co. vs. Teleflex, Inc.*, 127 S.Ct. 1727 (2007) (Kennedy, J.), the Court explained that "[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." The Court further required that an explicit analysis for this reason must be made.

"[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR 127 S.Ct.* at 1741, quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006).

In the instant case, Applicant respectfully submits that there are significant differences between the cited references and the claimed invention and there is no apparent reason to combine the known elements in the manner as claimed, and thus no *prima facie* case of obviousness has been established. Further, even if DiGiorgio and Barlow were properly combinable their combination would still not teach or suggest Applicant's claim limitations.

DiGiorgio and Barlow, taken alone or in any combination, do not teach or suggest the following limitations: (1) the security computing device storing a serial number associated with the security computing device and a user key associated with the serial number that is unique to the security computing device in the secure memory…wherein when the computer attempts to log onto the server over the computer network, the server: (2) requests a serial number from the security computing device, (3) verifies whether the serial number received from the security computing device is stored as one of the plurality of registered serial numbers in the user information database, (4) obtains the associated user key and computes a challenge and computes an expected response based on the associated user key, the server sends the challenge to the security computing device over the computer network; (5) the security computing device computes a response based upon a user key stored in the secure memory of the security computing device; and (6) based upon a request from the computer for an asset, the server to encrypt the asset with an asset key and to encrypt the asset key with the user key of the security computing device and to send the encrypted asset and asset key to the computer; as recited in claims 1 and 14.

DiGiorgio teaches that each user has a globally unique ID that is encoded on the secure token device (DiGiorgio, col. 10, lines 54-55). DiGiorgio does not teach or suggest a security computing device that *stores a serial number associated with the security computing device in a secure memory*, as recited in claims 1 and 14. In DiGiorgio, the secure token device holds user identification information that is globally unique and contains personal information regarding a user, such as name, address, and credit card account information (DiGiorgio, col. 2, lines 58-60).

In contrast, a *serial number* is a unique number assigned by the vendor to each unit of hardware or software (Computer Desktop Encyclopedia, 2d Edition, "serial number"). As set forth in Applicant's patent application, serial number 386 of the security device 110 is sealed in the secure memory 379 of the security device 110 during manufacturing and thereafter can no longer be written over once the secure memory 379 is sealed (Detailed Description, page 51, lines 11-17). Thus, the serial number 386 is a unique number assigned during manufacturing to the security device 110.

DiGiorgio does not teach or suggest *storing a serial number associated with the security computing device in a secure memory.*

DiGiorgio teaches that the ISP issues a challenge to the secure token device 10 to ensure that the user should be granted access to ISP services (DiGiorgio, col. 10, lines 31-33), DiGiorgio does not teach or suggest the server *requesting a serial number from the security computing device*...the security computing device to transmit *the serial number from the secure memory*, as recited in claims 1 and 14. As set forth in Applicant's patent application, the server 104 requests a serial number 386, stored in the secure memory 379 of the security device 110 from the security device 110 (Detailed Description, page 53, lines 9-11).

The challenge-response scheme of DiGiorgio and the use of the User ID therein relied upon by the Examiner quite simply does not teach or suggest Applicant's limitations related to a server *requesting a serial number from the security computing device*...the security computing device to transmit *the serial number from the secure memory*.

In fact, Applicant's claimed challenge-response scheme does not even begin until the serial number is verified by the server, as will be described.

Moreover, Applicant can find no teaching or suggestion in DiGiorgio that the server verifies whether *the serial number received from the security computing device is stored as one of the plurality of registered serial numbers in the user information database*, as recited in claims 1 and 14.

Applicant quite simply can find no teaching or suggestion in the citations pointed to by the Examiner that the ISP of DiGiorgio verifies a *serial number* received from a security computing device is stored as one of a plurality of *registered serial numbers* in a *user information database*, as recited in claims 1 and 14. In fact, Applicant can find no teaching in DiGiorgio of an ISP coupled to a user information database containing a plurality of registered serial numbers. Applicant respectfully requests that the Examiner point to such a teaching.

Further, DiGiorgio does not teach or suggest the security computing device computing a response *based upon a user key stored in the secure memory of the security computing device*, as recited in claims 1 and 14. As described, in Applicant's patent application, the server 104 sends the challenge to the security device 110 and waits for the response from the security device 110 (Detailed Description, page 54, line 6-7). Both the server 104 and the security device 110 utilize the same mathematical transformation and have the same user key 387 such that the response generated at the security device 110 should be the same as the expected response created at the server 104 (Detailed Description, page 53, line 26 to page 54, line 2).

In contrast, Applicant can find no teaching DiGiorgio of a security computing device computing a response based upon a user key stored in the secure memory of the security computing device. Applicant respectfully requests that the Examiner point to such a teaching.

As to Barlow, Barlow merely discloses a commerce application running at the merchant's computer receiving a signed encrypted order and passing the package to its own cryptography services module 40 (Barlow, col. 17, lines 59-62). The signed encrypted order is transmitted from the user's computer over the network to the merchant's computer (Barlow, col. 17, lines 55-57). The order disclosed in Barlow is a purchase order in an electronic shopping context (Barlow, col. 4, lines 36-41). The order, generated by the commerce application, is approved by the user and encrypted in order to be securely transmitted over the open and insecure public network (Barlow, col. 16, lines 39-40).

There is no teaching or suggestion in Barlow of, based upon a request from the computer for an asset, the *server to encrypt an asset with an asset key and to encrypt the asset key with the user key of the security computing device and to send the encrypted asset and asset key to the computer*, as recited in claims 1 and 14. By way of background, as described in Applicant's patent application, the asset database 107 is coupled to the server 104 (Detailed Description, page 48, lines 5-8) and contains assets (e.g. multimedia presentations associated with musical pieces, audio files, as well as other digital data assets) and unique asset encryption keys for each asset (Detailed Description, page 49, lines 18-22). Each asset is uniquely encrypted with a different, unique asset key particularly for that asset, utilizing the security software module 422 of the server 104. The asset key for the asset is encrypted using the user key of the associated security device 100 of the requesting computing device 102 (Detailed Description, page 61, lines 13-20). The encrypted asset 905 and the encrypted asset key 909 are sent to the computing device 102 where it is stored in memory (Detailed Description, page 62, lines 12-17).

Although, Barlow teaches encrypted orders being supplied to the CAPI 42 for purposes of being decrypted and verified (Barlow, col. 17, lines 62-64). Barlow does not teach or suggest *a server encrypting an asset with an asset key*, as recited in claims 1 and 14.

Further, although Barlow teaches that the CAPI 42 passes the encrypted order to the CSP 44 for decryption (Barlow, col. 18, lines 3-5)...and that the CAPI 42 passes the encrypted order to the CSP 44 for decryption using the merchant's private key exchange key, (Barlow, col. 18, lines 3-8), Applicant respectfully submits that this is no way teaches or suggests *encrypting an asset with an asset key and encrypting the asset key with a user key of a security computing device and sending the encrypted asset and asset key to the computer*.

These limitations are quite clearly not taught or suggested by Barlow.

Applicant respectfully submits that even if there were a sufficient motivation or reason to combine DiGiorgio with Barlow, as previously described, their combination would still not teach or suggest the novel and non-obvious claim limitations as set forth in Applicant's independent claims 1 and 14.

Therefore, Applicant respectfully requests that the Examiner allow Applicant's independent claims 1 and 14. Applicant respectfully submits that the dependent claims are allowable for being dependent from allowable independent claims.

Conclusion

In view of the remarks made above, it is respectfully submitted that pending claims 1, 4, 9-14, 17, and 22-26 are allowable over the prior art of record. Thus, Applicant respectfully submits that all the pending claims are in condition for allowance, and such action is earnestly solicited at the earliest possible date. The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application. To the extent necessary, a petition for an extension of time under 37 C.F.R. is hereby made. Please charge any shortage in fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: November 19, 2007 By____________________
Eric T. King
Reg. No. 44,188
Tel.: (714) 557-3800 (Pacific Coast)

12400 Wilshire Boulevard, Seventh Floor
Los Angeles, California 90025

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING	FACSIMILE
□ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*	☒ *transmitted by facsimile to the Patent and Trademark Office.*
Date: November 19, 2007	__________ November 19, 2007 *Tu Nguyen* *Date*